(12) UK Patent Application (19) GB (11) 2 362 061 (13) A

(43) Date of A Publication 07.11.2001

(21) Application No 0009050.6

(22) Date of Filing 12.04.2000

(71) Applicant(s)
3Com Corporation
(Incorporated in USA - Delaware)
5400 Bayfront Plaza, M/S 1308, Santa Clara,
California 95052-8145, United States of America

(72) Inventor(s)
David James Stevenson
Robert James Duncan
Alastair Hugh Chisholm
Ronan Francois Daniel Grandin
Neil William Gray

(74) Agent and/or Address for Service
Brookes Batchellor
102-108 Clerkenwell Road, LONDON, EC1M 5SA,
United Kingdom

(51) INT CL⁷
H04Q 3/00 , H04L 12/26

(52) UK CL (Edition S)
H4K KFMA

(56) Documents Cited
US 5751964 A

(58) Field of Search
UK CL (Edition R) H4K KFM , H4P PEUX PFD
INT CL⁷ H04L 12/24 12/26 , H04Q 3/00
ONLINE: WPI, EPODOC, JAPIO.

(54) Abstract Title

Network management apparatus and method using an adjustable threshold

(57) A network management method for use in adjusting a threshold value for a monitored characteristic of a managed network comprises comparing one or more values obtained during previous monitoring of the characteristic against an adjusted threshold value, and compiling a list of the values which exceed the adjusted threshold value. The method creates a list which the network administrator can use during adjustment of threshold values. In one embodiment, the method is implemented in the from of a computer program.

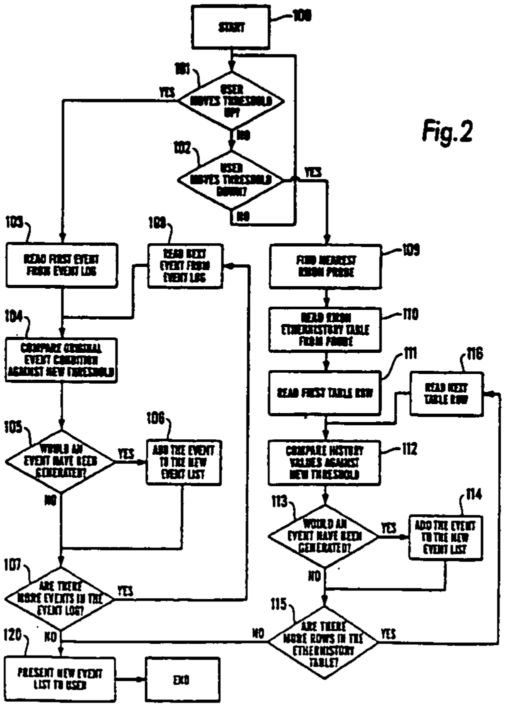
START
100
101
USER MOVES THRESHOLD UP?
YES
NO
102
USER MOVES THRESHOLD DOWN?
YES
NO
103
READ FIRST EVENT FROM EVENT LOG
108
READ NEXT EVENT FROM EVENT LOG
109
FIND NEAREST RMON PROBE
104
COMPARE ORIGINAL EVENT CONDITION AGAINST NEW THRESHOLD
110
READ FROM ETHERHISTORY TABLE FROM PROBE
111
READ FIRST TABLE ROW
116
READ NEXT TABLE ROW
105
WOULD AN EVENT HAVE BEEN GENERATED?
YES
NO
106
ADD THE EVENT TO THE NEW EVENT LIST
112
COMPARE HISTORY VALUES AGAINST NEW THRESHOLD
113
WOULD AN EVENT HAVE BEEN GENERATED?
YES
NO
114
ADD THE EVENT TO THE NEW EVENT LIST
107
ARE THERE MORE EVENTS IN THE EVENT LOG?
YES
NO
115
ARE THERE MORE ROWS IN THE ETHERHISTORY TABLE?
NO
YES
120
PRESENT NEW EVENT LIST TO USER
END

Fig.2

GB 2 362 061 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

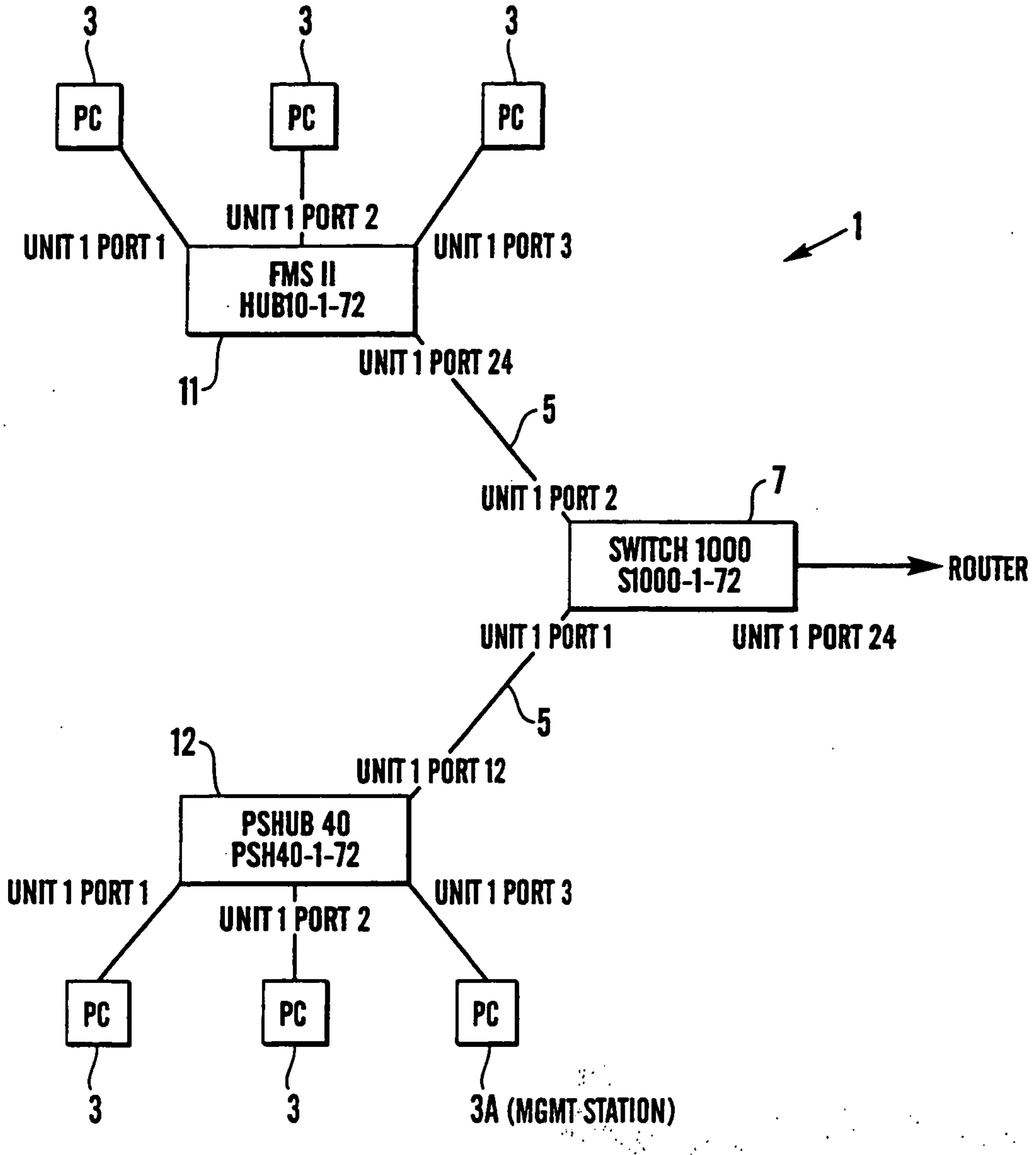
3
3
3
PC
PC
PC
UNIT 1 PORT 2
UNIT 1 PORT 1
UNIT 1 PORT 3
1
FMS II
HUB10-1-72
11
UNIT 1 PORT 24
5
7
UNIT 1 PORT 2
SWITCH 1000
S1000-1-72
ROUTER
UNIT 1 PORT 1
UNIT 1 PORT 24
5
12
UNIT 1 PORT 12
PSHUB 40
PSH40-1-72
UNIT 1 PORT 1
UNIT 1 PORT 2
UNIT 1 PORT 3
PC
PC
PC
3
3
3A (MGMT STATION)

Fig. 1

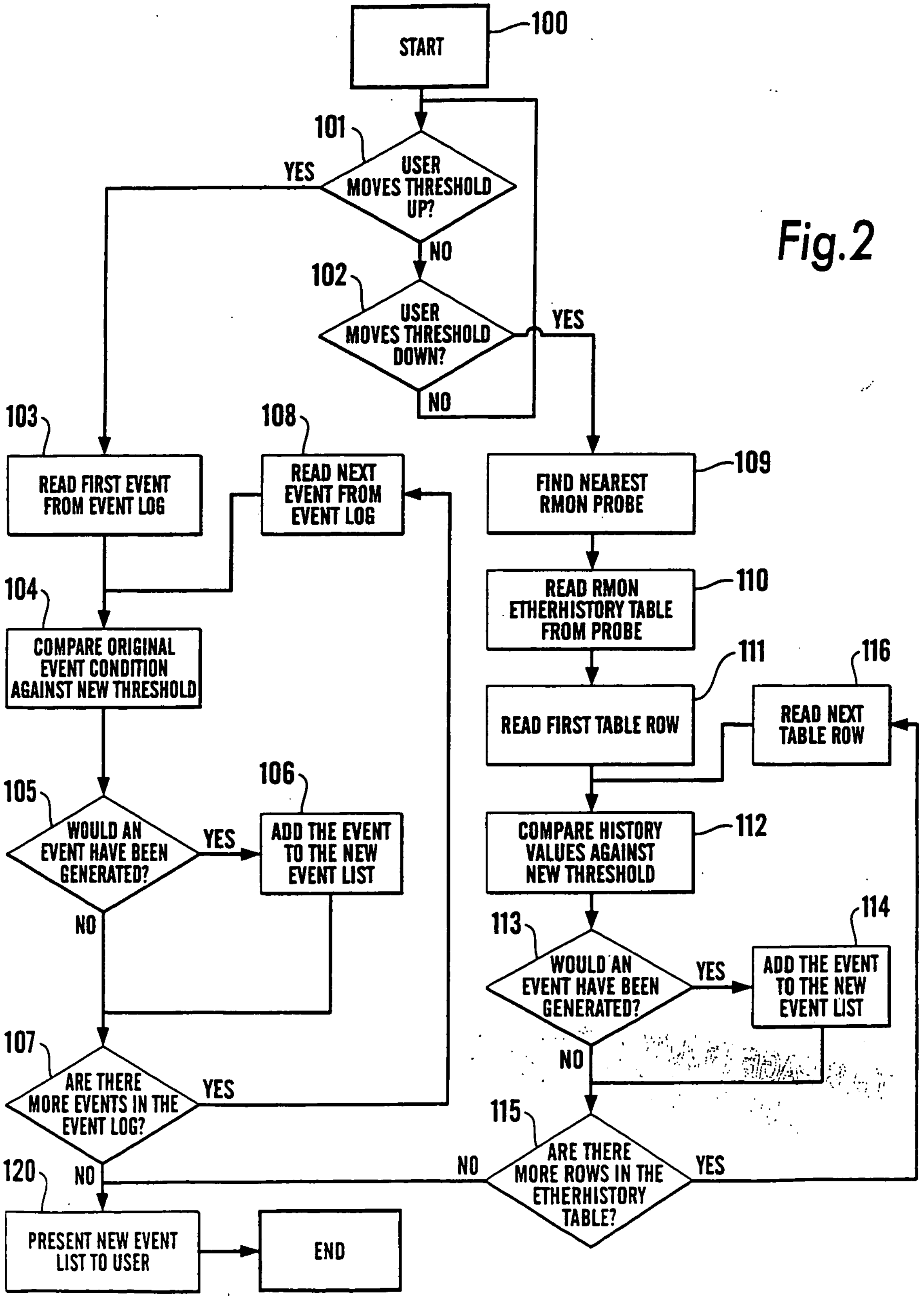
START
100
101
USER MOVES THRESHOLD UP?
YES
NO
102
USER MOVES THRESHOLD DOWN?
YES
NO
103
READ FIRST EVENT FROM EVENT LOG
108
READ NEXT EVENT FROM EVENT LOG
104
COMPARE ORIGINAL EVENT CONDITION AGAINST NEW THRESHOLD
105
WOULD AN EVENT HAVE BEEN GENERATED?
YES
NO
106
ADD THE EVENT TO THE NEW EVENT LIST
107
ARE THERE MORE EVENTS IN THE EVENT LOG?
YES
NO
120
PRESENT NEW EVENT LIST TO USER
END
109
FIND NEAREST RMON PROBE
110
READ RMON ETHERHISTORY TABLE FROM PROBE
111
READ FIRST TABLE ROW
116
READ NEXT TABLE ROW
112
COMPARE HISTORY VALUES AGAINST NEW THRESHOLD
113
WOULD AN EVENT HAVE BEEN GENERATED?
YES
NO
114
ADD THE EVENT TO THE NEW EVENT LIST
115
ARE THERE MORE ROWS IN THE ETHERHISTORY TABLE?
NO
YES

Fig.2

NETWORK MANAGEMENT APPARATUS AND METHOD FOR MONITORING STRESS IN A NETWORK

The present invention relates generally to an apparatus and method for the management of a network, and more particularly to a network management apparatus and method for monitoring the health or stress of a network.

The following description is concerned with a data communications network, and in particular a local area network (LAN) but has more widespread applicability to other managed communications systems including wide area networks (WANs) or wireless communications systems.

Networks typically comprise a plurality of computers, peripherals and other electronic devices capable of communicating with each other by sending and receiving data packets in accordance with a predefined network protocol. Each computer or other device on the network is connected by a port to the network media, which in the case of a LAN network may be coaxial cable, twisted pair cable or fibre optic cable. Each device on the network typically has hardware for media access control (MAC) with its own unique MAC address. Data packets are sent and received in accordance with the MAC protocol (e.g. CSMA/CD protocol as defined by the standard IEEE 802.2, commonly known as Ethernet). Data packets transmitted using the MAC protocol identify the source MAC address (i.e. the MAC address of the device sending the data packet) and the destination MAC address (i.e. the MAC address of the device for which the data packet is destined) in the header of the data packet.

A network is generally configured with core devices having a plurality of ports, which can be used to interconnect a plurality of media links on the network. Such devices include hubs, routers and switches which pass data packets received at one port to one or more of its other ports, depending upon the type of device. Such core devices can either be managed or unmanaged.

A managed device is capable of monitoring data packets passing through its ports. For example, a managed device can learn the physical or MAC addresses of the devices connected to its ports by monitoring the source address of data packets passing through the respective ports. Identified source addresses transmitted from a port of a managed network device, such as a router, hub, or switch, are stored in a respective "address table" associated with the port

Managed devices additionally have the capability of communicating with each other using a management protocol such as the SNMP (Simple Network Management Protocol), as described in more detail below. Whilst the following description is concerned with the SNMP management protocol, the skilled person will appreciate that the invention is not limited to use with SNMP, but can be applied to managed networks using other network management protocols.

SNMP defines agents, managers and MIBs (where MIB is Management Information Base), as well as various predefined messages and commands for data communication. An agent is present in each managed network device and stores management data, responds to requests from the manager using the GETRESPONSE message and may send a TRAP message to the manager after sensing a predefined condition. A manager is present within the network management station of a network and automatically interrogates the agents of managed devices on the network using various SNMP commands such as GET and GETNEXT commands, to obtain information suitable for use by the network administrator, whose function is described below. A MIB is a managed "object" database which stores management data obtained by managed devices, and is accessible to agents for network management applications.

SNMP forms part of the TCP/IP protocol suite, which is a number of associated protocols developed for networks connected to the Internet also known as the World Wide Web.

It is becoming increasingly common for an individual, called the network administrator, to be responsible for network management, and his or her computer system or workstation is typically designated the network management station. The network management station incorporates the manager, as defined in the SNMP protocol, i.e. the necessary hardware, and software applications to retrieve data from MIBs by sending standard SNMP requests to the agents of managed devices on the network.

Network management software applications are known which can determine the topology of a network, i.e. the devices on the network and how they are linked together. In order to determine the network topology, the application retrieves data from the managed devices on the network, which data can provide information about the devices connected to the managed devices, for instance the aforementioned "address tables". MIB data can also be retrieved from managed devices to provide information about device type, device addresses and details about the links. Using such data, the application can usually determine the topology of the entire network.

An example of a known network management software application capable of determining network topology is the Transcend® Network Supervisor application available from 3Com Corporation of Santa Clara, California, USA.

A part of the network administrator's function is to identify and resolve problems occurring on the network, such as device or link malfunction or failure. In order to provide the network administrator with the necessary information to identify such problems, the network management application monitors the devices on the network. An example of such monitoring is described in co pending UK Patent Application No 9917993.9 entitled "Management System and Method for Monitoring Stress in a Network" in the name of the present applicant. In the system and method described in UK Patent Application No 9917993.9 the SNMP manager in the network management station requests the agents of managed network devices on the network device to retrieve selected MIB data indicative of device and link operation, and performs tests for device activity and service availability. Such MIB data may relate to characteristics such as traffic activity or errors occurring at a particular port in the relevant network device. Tests may include sending ICMP Ping requests to each device on the network, or sending selected requests for services such as SMTP, NFS and DNS to servers, and monitoring the time taken to receive a response. The monitored parameters or characteristics are referred to herein as "stress metrics".

The network management application compares, for each stress metric, the retrieved data or test results against a corresponding threshold level for the stress metric. The threshold level is the level above (or below) which performance is considered to be unacceptable. For simplicity, the following description is based on a maximum threshold, that is a threshold level above which performance is considered to be unacceptable. The skilled person will appreciate that for some stress metrics the threshold level could be a level below which performance is unacceptable. Default values for threshold levels of monitored stress metrics are typically preset by the application vendor, but may be adjusted by the network administrator.

Each time a threshold is exceeded, the application logs an "Event". The "Event log" lists each Event, and includes information such as the date and time of the Event, the identity of the device affected and the nature of the Event. The network administrator can then review the Event list to identify problems on the network.

It is important that the thresholds for the monitored stress metrics are chosen so that the number of Events presented in the Event log for review is minimised whilst still keeping the network administrator informed of Events which indicate genuine problems on the network for which he is responsible. It can be difficult for the network administrator to choose a threshold level which will be exceeded only if genuine problems exist on his particular network. Accordingly, there is a need for a system and method which can be employed by the network administrator to assist in setting the threshold levels.

In accordance with a first aspect, the present invention provides a method for use in adjusting a threshold value for a monitored characteristic of a managed network, the method comprising the steps of: receiving an adjusted threshold value; comparing one or more values obtained during previous monitoring of the characteristic against the adjusted threshold value; and compiling a list of data relating to said values which exceed the adjusted threshold value.

The present invention thus produces a simulated list of past Events which would have been previously recorded in an Event log had the threshold been set at the adjusted threshold level. This enables the network administrator to make an informed decision about the adjustment of thresholds. Advantageously, the setting of the threshold level is tailored to suit the operating characteristics of the individual network concerned, by using data generated during previous operation of the network.

In one embodiment, the method comprises: adjusting said stress threshold up; comparing previously recorded stress levels obtained during monitoring of the characteristic from an Event log against the adjusted threshold; and storing data for those previously recorded stress values which would have exceeded the adjusted threshold in the list. The method further comprises presenting the list of retained previously recorded stress values for review by the network administrator

In another embodiment, the method comprises: adjusting said stress threshold down; retrieving historical data from a managed network device on the network, the historical data relating to stress levels for the monitored characteristic; comparing stress values in the historical data against the adjusted threshold, and storing data relating to the stress values which exceed the adjusted threshold. The data is then provided for review by the network administrator.

In accordance with a second aspect, the present invention provides a computer readable medium carrying a computer program for carrying out the method of the first aspect of the present invention.

In accordance with a third aspect, the present invention provides a network management apparatus for carrying out the method in accordance with the first aspect of the present invention.

Further preferred features and advantages of the present invention will be apparent from the following description and accompanying claims.

Embodiments of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a typical network having a network management station in accordance with the present invention, and

Figure 2 is a flow chart showing the steps carried out by a computer program in accordance with a preferred embodiment of the present invention.

Figure 1 shows a typical network 1 incorporating a network management system according to a preferred embodiment of the present invention. The network 1 includes a network management station 3A which incorporates the necessary hardware and software for network management. In particular, the network management station includes a processor, a memory and a disk drive as well as user interfaces such as a keyboard and mouse, and a visual display unit. Network management application software in accordance with the present invention is loaded into the memory of management station 3A for processing data as described in detail below. The network management station 3A is connected by network media links 5 to a plurality of managed network devices including core devices such as network switch 7, hubs 11 and 12, and a router (not shown), which may be managed or unmanaged, and end stations including personal computers 3 and workstations. The network may also include unmanaged devices, for example peripheral devices such as printers.

The network management station 3A is capable of communicating with the managed network devices such as network switch 7 and hubs 11 and 12 by means of a network management protocol, in the present embodiment the SNMP protocol, in order to obtain network management data. Each managed device includes a processor which monitors operational characteristics and an SNMP agent which stores the monitored data as MIB data in memory on the device as is well known in the art, including data relating to *inter alia* data traffic at the device.

An SNMP managed device may monitor data for a number of MIBs. An example of a MIB containing network management data is MIB-II (formerly MIB-I) as specified by the IETF (Internet Engineering Task Force) in specification RFC1213. MIB-II is common to most vendors' core devices and any network management system should preferably be capable of reading and utilising management data from MIB-II. Furthermore, the network management system of the preferred embodiment of the present invention is additionally capable of reading and utilising more complex management data contained in such MIBs as RMON (Remote Monitoring MIB, RFC1271), RMON2 (Remote Monitoring MIB 2, RFC2021), the standard bridge MIB (RFC1493), the standard repeater MIB (RFC1516), or any proprietary MIBs produced by original equipment manufacturers (e.g. the 3Com Remote Poll MIB).

In network 1, hubs 11 and 12 and switch 7 are MIB-II compatible, and switch 7 is also RMON compatible.

In accordance with the preferred embodiment of the present invention, the network management station 3A monitors a plurality of stress metrics. The stress levels or values for the metrics are obtained by periodically requesting relevant MIB-II data from hubs 11 and 12 and switch 7, and RMON data from switch 7, and by periodically polling all network devices using Ping or service requests and monitoring response times.

The network management station 3A compares each monitored stress level against a corresponding predetermined threshold level for the stress metric. Each time a threshold is exceeded, the network management station 3A stores details about the monitored stress level in an Event log in memory. Monitored stress levels which do not exceed the threshold are not stored in the Event log and the received data about these monitored levels is discarded or overwritten by subsequent monitored stress levels.

A typical Event log is shown in Table 1 below. Each Event listed in the Event log represents a monitored stress level which exceeded the threshold set for the stress metric at the time of the Event.

Table 1

Time	Device Name	Device Type	Description
11.06	HUB10-1-72	FMS II	Utilisation on port 2 exceeded 80%
11.00	S1000-1-72	SWITCH 1000	Errors on port 24 exceeded 5%
10.58	S1000-1-72	SWITCH 1000	Errors on port 2 exceeded 5%
10.58	PSH40-1-72	PSHUB 40	Broadcasts on port 12 exceeded 200/s
10.57	HUB10-1-72	FMS II	Utilisation on port 2 exceeded 80%
10.56	S1000-1-72	SWITCH 1000	Utilisation on port 24 exceeded 80%

The threshold for each metric is preset in the network management station 3A and is adjustable by the network administrator. The network administrator conventionally has no means of establishing the appropriate threshold level for the monitored stress metrics to ensure that he or she is informed of all genuine Events, i.e. Events indicative of genuine problems on the network, but is not notified of Events which are not significant for the network concerned.

In accordance with a preferred embodiment of the present invention, the network management station 3A operates a method which uses data obtained during previous monitoring of the network to simulate an Event log in accordance with one or more adjusted thresholds. The network administrator can use the method to try a number of different adjusted threshold levels for each stress metric and choose the most suitable level which records only genuine Events.

The method of the present invention is preferably implemented in a computer program. In accordance with the preferred embodiment, the computer program carries out the steps illustrated in Figure 2.

The program is initiated by the network administrator (the user) changing a threshold value, which triggers the program to start at 100. At step 101 the program considers whether the threshold has been increased. This may be done by comparing the new threshold value with the original threshold value for the stress metric concerned. If the new threshold is greater than the original threshold then the program determines that the threshold has increased. If the program determines in step 101 that the threshold level has been increased by the user, the program continues with a first program branch according to steps 103 to 108, described in more detail below. If step 101 determines that the threshold level has not been increased, in step 102 the program considers whether the threshold has been reduced. If the program determines in step 102 that the threshold level has been decreased by the user, the program continues with a second program branch according to steps 109 to 116, described in more detail below.

The first program branch is performed in response to an increase in a threshold value. This branch uses the existing log of Events of the network management application, as described above, to produce a simulated, new list of past Events, which would have been logged with the increased threshold value.

At step 103, the program reads the data for the first Event in the existing Event log. The first Event is typically the most recent Event, although the order of Events in the Event log is dependent on the network management application and/or the administrator and is not significant in the context of the present invention. The Event data includes the monitored stress value, which exceeded the original threshold and triggered the Event, referred to herein as the "Event condition".

In step 104 the program compares the Event condition against the new threshold. In step 105 the program determines whether the Event condition would have generated an Event if the threshold had been set at the new threshold. Thus, if the stress value causing the Event was found in step 104 to be greater than or equal to the new threshold, in step 105, the program determines that an Event would have been generated, in which case the program stores the Event data in the new Event list at step 106 and continues with step 107. If the stress value causing the Event was found in step 104 to be less than the new threshold, in step 105, the program determines that an Event would not have been generated and goes straight to step 107.

In step 107, the program considers whether there are any more Events in the original Event log. If there exist more Events in the Event log, the program continues by reading the next Event at step 108. The program continues with steps 104 to 107, until step 107 determines that no more Events exist. The program then continues with step 120 by presenting the new Event list. The program then ends.

The second program branch is performed in response to a decrease in a threshold value. This branch uses both the existing log of Events of the network management application, as described above, and further retrieved management data to produce a simulated, new list of Events, which would have been logged with the reduced threshold value.

In step 109, the program determines the managed network device which is nearest to the device or link being monitored by the metric, and which stores suitable historical data for the metric. The managed network device may be a specialised monitoring device or may be a core managed network device such as a hub or switch. In the preferred embodiment, the historical data is monitored and stored by an "RMON probe", as is well known in the art, and is made available by it through the

RMON etherHistory MIB table. It will be appreciated that other management probes may be used for the same purpose. Accordingly, in the preferred embodiment, the program determines in step 109 the nearest RMON probe to the device or link monitored by the metric. This is achieved using knowledge of the network topology.

Once the nearest RMON probe has been determined; in step 110 the program reads the etherHistory table from the RMON probe. The table is read by retrieving rows of the table using the GET or GETNEXT SNMP commands.

Having retrieved the table, the program continues at step 111 by reading the first row in the table which includes the stress value(s) for the stress metric, as monitored by the RMON probe.

In step 112 the program compares the or each stress value or "history value" of the first table row with the new threshold. In step 113 the program determines whether the history value would have generated an Event if the threshold had been set at the new threshold. Thus, if the history value was found in step 112 to be greater than or equal to the new threshold, in step 113, the program determines that an Event would have been generated, in which case the program at step 114 generates an Event based on the history value, and stores this Event in the new, simulated Event list, which includes a copy of all the Events from the existing Event log and continues with step 115. If the history value was found in step 112 to be less than the new threshold, in step 113, the program determines that an Event would not have been generated and goes straight to step 115.

In step 115, the program considers whether there are any more rows in the MIB table. If more rows exist, the program continues by reading the next row in the table at step 116. The program continues with steps 112 to 115 until step 115 determines that no more table rows exist. The program then continues with step 120 by presenting the new Event list. The program then ends.

It will be appreciated that program steps 101 and 102 may be included in a single step and the program could be initiated by the program automatically selecting adjusted threshold values. Furthermore, it will be appreciated that to produce the new Event list using the first branch, the existing Event log could be copied and Events removed from the Event log if step 105 determines that the Event would not have been generated. In that case, step 106 would not be employed.

Various modifications may be made to the described embodiments. It is intended to include all such modifications and changes which fall within the scope of the present invention as defined in the accompanying claims.

CLAIMS:

1. A method for use in adjusting a threshold value for a monitored characteristic of a managed network, the method comprising the steps of: receiving an adjusted threshold value for the monitored characteristic; comparing one or more values obtained during previous monitoring of the characteristic against the adjusted threshold value, and compiling a list of data relating to said values which exceed the adjusted threshold value.

2. A method as claimed in claim 1, wherein the monitored characteristic is indicative of the performance of the network or a part thereof, and the threshold value is a value above which performance is deemed to be unacceptable.

3. A method as claimed in claim 1 or claim 2, wherein the one or more values obtained during previous monitoring are values which exceeded an unadjusted threshold value previously stored in memory.

4. A method as claimed in claim 3, wherein the step of adjusting comprises increasing the threshold value.

5. A method as claimed in claim 3 or claim 4, wherein the step of comparing comprises reading each of said one or more values in turn, and comparing each value with the adjusted threshold value.

6. A method as claimed in claim 5, wherein the step of compiling comprises storing data relating to each of said one or more values which exceed the adjusted threshold value as the list.

7. A method as claimed in claim 5, wherein the step of compiling comprises copying the one or more values from memory into said list, and removing from the list each of said one or more values which do not exceed the adjusted threshold.

8. A method as claimed in claim 1 or claim 2, wherein the one or more values obtained during the previous monitoring are historical values stored by a managed device on the network.

9. A method as claimed in any one of claim 8, wherein the step of adjusting comprises decreasing the threshold value.

10. A method as claimed in claim 8 or claim 9, wherein the step of comparing comprises reading each of said one or more values in turn, and comparing each value with the adjusted threshold value.

11. A method as claimed in claim 8, 9 or 10, wherein, before the step of comparing, the method comprises retrieving said historical values stored by said managed network device on the network.

12. A method as claimed in claim 11, wherein, before the step of retrieving, the method comprises determining the managed device containing historical values for the monitored characteristic which is nearest to the part of the network being monitored using knowledge of the topology of the network.

13. A method as claimed in claim 11 or claim 12, wherein the historical values are stored in SNMP MIBs and are retrieved using SNMP commands.

14. A method as claimed in claim 13, wherein the managed network device is an RMON probe and the historical values are stored in the RMON etherHistory table.

15. A method as claimed in any one of claims 8 to 14, wherein the step of compiling comprises storing data relating to each of said one or more values which exceed the adjusted threshold in said list.

16. A method as claimed in claim 15, wherein the step of compiling further comprises retrieving data relating to values obtained during previous monitoring which exceeded an unadjusted threshold value from memory, and storing said data in the list.

17. A method as claimed in any preceding claim wherein the data relating to said values comprises information including one or more of: the time the value was monitored; the monitored device; the monitored characteristic, and the monitored value.

18. A method as claimed in any preceding claim, further comprising presenting said compiled list to a user.

19. A method for use in adjusting a threshold value for a monitored characteristic of a managed network substantially as hereinbefore described with reference to, and as shown, Figure 2 of the accompanying drawings.

20. A computer readable medium including a computer program for carrying out the method as claimed in any one of claims 1 to 19.

21. Apparatus for use in adjusting a threshold value for a monitored characteristic of a managed network, the apparatus comprising means for receiving an adjusted threshold value for a monitored characteristic; means for comparing one or more values obtained during previous monitoring of the characteristic against the adjusted threshold value, and means for compiling a list of said one or more values which exceed the adjusted threshold value.

CHARTER MARK

PATENTS • DESIGNS • The Patent Office • COPYRIGHT • TRADE MARKS

INVESTOR IN PEOPLE

16

Application No:	GB 0009050.6	**Examiner:**	Stephen Brown
Claims searched:	1-21	**Date of search:**	13 October 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): H4P (PFD, PEUX), H4K (KFM).

Int Cl (Ed.7): H04L: 12/24, 12/26, H04Q: 3/00.

Other: Online: WPI, EPODOC. JAPIO.

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	US 5 751 964 (IBM)	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
		E	Patent document published on or after, but with priority date earlier than, the filing date of this application.
&	Member of the same patent family		